99TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPT. 99-753
Part 1

COMPUTER SECURITY ACT OF 1986

AUGUST 6, 1986.—Ordered to be printed

Mr. FUQUA, from the Committee on Science and Technology, submitted the following

NEWARK PUBLIC LIBRARY
AUG 25 1986
U. S. GOVT. PUBS.
DEPOSITORY 376

REPORT

together with

ADDITIONAL AND DISSENTING VIEWS

[To accompany H.R. 2889 which on June 27, 1985, was referred jointly to the Committee on Science and Technology and the Committee on Government Operations]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science and Technology, to whom was referred the bill (H.R. 2889) to amend the Act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems, having considered the same, report favorably thereon with amendments and recommend that the bill as amended do pass.

The amendments are as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1986".

SEC. 2. PURPOSE.

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.—The purposes of this Act are—

(1) to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including standards and guidelines needed to assure the cost-effective security and privacy of sensi-

71-006 O

Y1.1/8:

tive information in Federal computer systems, by amending the Act of March 3, 1901;

(2) to provide for promulgation of such standards and guidelines by amending section 111(f) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended—

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof a semicolon, and by inserting after such paragraph the following:

"(20) the study of equipment, procedures, and systems for automatic acquisition, storage, manipulation, display, and transmission of information, and its use to control machinery and processes.";

(2) by redesignating section 18 as section 20, and by inserting after section 17 the following new sections:

"SEC. 18. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce, for promulgation under section 111 of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1986; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1986;

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) As used in this section and section 19, the terms 'computer system', 'Federal computer system', 'operator of a Federal computer system', and 'sensitive information' have the meanings given in section 7 of the Computer Security Act of 1986.

"SEC. 19. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency."; and

(3) by adding at the end thereof the following new section:

"SEC. 21. This Act may be cited as the National Bureau of Standards Act.".

SEC. 4. AMENDMENT TO BROOKS ACT.

(a) AMENDMENT.—Section 111(f) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(f)) is amended to read as follows:

"(f)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 18(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems.

"(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be promptly transmitted to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate.

"(4) The Administrator shall ensure that such standards and guidelines are implemented within an integrated information resources management system (as required by chapter 35 of title 44, United States Code) by—

"(A) developing and implementing policies on Federal computer systems; and

"(B) revising the Federal information resources managment regulations (41 CFR ch. 201) to implement such standards, guidelines, and policies.

"(5) As used in this section, the terms 'computer system', 'operator of a Federal computer system', and 'Federal computer system' have the meanings given in section 7 of the Computer Security Act of 1986.".

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 111 of such Act is further amended—

(1) by striking out "automatic data processing equipment" and "automatic data processing systems" each place they appear and inserting in lieu thereof "computer systems"; and

(2) by striking out "Automatic data processing equipment" and inserting in lieu thereof "Computer systems".

SEC. 5. TRAINING BY OPERATORS OF FEDERAL COMPUTER SYSTEMS.

(a) IN GENERAL.—Each operator of a Federal computer system that contains sensitive information shall provide mandatory periodic training in computer security awareness and accepted computer security practice. Such training shall be provided under the guidelines developed pursuant to section 18(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section, for all employees who are involved with the management, use, or operation of computer systems.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR OPERATORS OF FEDERAL COMPUTER SYSTEM FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each operator of a Federal computer system shall identify each computer system, and system under development, of that operator which contains sensitive information. In the case of a Federal contractor or

READEX FICHE best copy available

other organization (operating a Federal computer system), such identification shall be reviewed and approved by its supervising Federal agency.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such operator shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of the computer systems identified pursuant to subsection (a). Copies of such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. In the case of a Federal contractor or other organization (operating a Federal computer system), such plan shall be transmitted through its supervising Federal agency. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget.

SEC. 7. DEFINITIONS.

As used in this Act, sections 18 and 19 of the National Bureau of Standards Act, and section 111 of the Federal Property and Administrative Services Act of 1949—

(1) the term "computer system" means any equipment or interconnected collection of equipment, including—

(A) ancillary equipment;

(B) software and other procedures;

(C) services; and

(D) other resources,

that are used in the automatic acquisition, storage, manipulation, or display, or in any associated electromagnetic transmission and reception, of information;

(2) the term "Federal computer system" means a computer system operated by a Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949) or by a contractor of a Federal agency or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function;

(3) the term "operator of a Federal computer system" means a Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949), contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function;

(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552 of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

SEC. 8. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to each Federal agency such sums as may be necessary for fiscal years 1987, 1988, and 1989 to carry out the computer systems security training program established by section 5 of this Act and the identification and planning requirements of section 6.

Amend the title so as to read:

A bill to amend the Act establishing the National Bureau of Standards to provide for a computer standards program within such Bureau, to provide for government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems.

CONTENTS

	Page
I. Background	6
II. Issues raised during the hearings	8
III. Need for legislation	15
IV. Explanation of the bill	15
V. Sectional analysis	22
VI. Effect of legislation on inflation	27
VII. Oversight findings and recommendations, Committee on Science and Technology	27

VIII. Oversight findings and recommendations, Committee on Government Operations 27
IX. Budget analysis and projection 28
X. Congressional Budget Office cost estimate 28
XI. Changes in existing law 31
XII. Committee recommendation 37
XIII. Additional views 38
XIV. Dissenting views 39

I. Background

Computers and information systems have so permeated today's society that there is virtually no sector which does not rely heavily on their use. This includes the Federal Government, which currently has over 17,000 medium- and large-scale computers and will have almost 500,000 microcomputers by 1990, according to a recent annual report by the General Services Administration, entitled "ADP Management of Information Systems," 1985.

The Federal Government is the largest single user of computers in the world. Its investment in automated systems technology is so large that about 1.6 percent of the 1986 budget will be spent on automated data processing (ADP) equipment and services, or more than 15 billion dollars. This budget includes ADP for defense and national security, education, national energy programs, social welfare, and tax programs (to name just a few).

As the role of the Federal Government has become broader, the need to automate and the corresponding need to secure data also has grown. In recent years, Congress and the executive agencies have directed their attention to Federal computer systems in a number of areas, including investigating and commenting on their integrity and security. Both Section 111(f) of the Federal Property and Administrative Services Act of 1949 (the Brooks Act of 1965) and the Paperwork Reduction Act of 1980 represented attempts by Congress to address the issues of automating information in Federal agencies and creating an efficient method of storing and disseminating this information. In October 1984, Congress passed the first Federal computer crime legislation. This law, the Counterfeit Access Device and Computer Fraud Act of 1984 (P.L. 98-473), prohibits unauthorized access into a Federal computer system to modify, destroy, or disclose information; unauthorized access to information to obtain financial or credit information protected by Federal financial privacy laws; and unauthorized access to obtain classified military intelligence information.

Within the Federal Government several agencies have been charged with the responsibility for establishing computer security controls and standards. The Office of Management and Budget (OMB) has overall responsibility for computer security policy. The General Services Administration (GSA) also issues regulations for physical security of computer facilities, and ensures that security hardware and software meet certain technological and fiscal specifications. In defense and national security, the National Security Agency (NSA) has traditionally been responsible for the security of classified information, including that processed by and stored within computers. Recently, NSA has been given the responsibility to establish and maintain technical standards for secure, or "trusted," computers. NSA does this through its administration of the

Department of Defense (DOD) National Computer Security Center. NSA also will work with industries at the DOD Computer Security Center to develop security standards for private sector use.

At the Department of Commerce, the National Bureau of Standards' (NBS') Institute of Computer Science and Technology (ICST) has developed computer and processing standards, such as the Data Encryption Standard (DES), which protects data transferred between automated information systems. The Federal Information Processing Standards (FIPS) developed by the ICST provide specific codes, language, procedures, and techniques for Federal and private sector information systems managers. Also at the Department of Commerce, the National Telecommunications and Information Administration (NTIA) has the responsibility for analyzing, developing, implementing and applying executive branch policy for telecommunications in the Federal Government.

CURRENT FEDERAL ROLE

This mixture of laws, regulations, and responsible agencies has raised concern that Federal computer security policy is lacking direction and forcefulness in some areas, yet has created overlapping and duplication of effort in other areas. Recently, Federal regulations and directives have been issued and congressional legislation has been introduced to address the lack of coordination of Federal ADP systems.

On March 15, 1985, OMB issued a draft circular intended "to provide a general framework of management of information resources." This circular combined and updated operative OMB circulars, including OMB Circular A-71 (originally issued in July 1978). A version of the draft circular was then included in a final OMB circular, A-130 (issued on December 12, 1985), in which Appendix III addressed Federal government computer security issues. Appendix III of A-130 is a very broad policy directive, outlining both intraagency and interagency guidelines for computer security. Those responsible for implementation of this circular include the Department of Commerce, Department of Defense, General Services Administration, and the Office of Personnel Management, in addition to OMB.

On September 17, 1984, the executive branch issued National Security Decision Directive 145 (NSDD-145), "National Policy on Telecommunications and Automated Information Systems Security." This directive is aimed at safeguarding automated information systems with a special focus on protecting those Federal systems accessed via (and dependent on) network communications. NSDD-145 creates a National Telecommunications and Information Systems Security Committee (NTISSC), a panel of 22 voting representatives from 12 defense/intelligence agencies and 10 civilian agencies. An Assistant Secretary of Defense chairs NTISSC, and the Director of the National Security Agency acts as the National Manager for implementing policy under NSDD-145. The NTISSC is empowered to issue operating policies to assure the security of telecommunications and automated information systems that process and communicate both classified national security information and other sensitive government information.

On June 27, 1985, Representative Dan Glickman, then chairman of the Subcommittee on Transportation, Aviation, and Materials, House Committee on Science and Technology, introduced H.R. 2889, the Computer Security Research and Training Act of 1985. This legislation would establish the NBS as the focal point for developing training guidelines for Federal employees who are involved in the management, operation, and use of automated information processing systems. This legislation was based in part on hearings which the subcommittee conducted in 1983 and a 1984 subcommittee report which had recommended increased ADP training and awareness in Federal agencies.

II. Issues Raised During the Hearings

The Subcommittee on Transportation, Aviation and Materials held a series of hearings which addressed computer and communications privacy and security in the Federal Government on September 24, 1984, June 27, 1985, and October 29 and jointly with the Subcommittee on Science, Research, and Technology on October 30, 1985. These hearings touched upon three major issues: (1) The current state of computer privacy and security in the Federal Government; (2) The major impact of NSDD–145 and the role of the NSA in setting Federal civilian computer security; (3) The role of the Federal Government in adequately training Federal employees and heightening awareness of computer security.

FEDERAL COMPUTER CRIME AND SECURITY

There has been a heightened awareness both inside and outside the Federal Government that current computer security measures are inadequate. This is an issue which has been discussed in congressional hearings since the mid-1970s, but it is only recently that several studies have attempted to quantify the extent of damage caused by computer fraud and abuse causes, as well as the demonstrated lack of computer preparedness and systems integrity in Federal ADP systems

During the September 24, 1984 hearings, John Tompkins, chairman of the Task Force on Computer Crime of the American Bar Association (ABA), commented on a survey conducted by the ABA on the state of computer crime in government and the private sector. The ABA report was one of the first extensive studies done on the number of "known and verifiable losses" which have resulted from computer crimes, and the results of the survey included responses from 13 Federal agencies and 28 State and local agencies. Although the results of the survey indicated a wide range of losses by respondents, several consistent factors emerged: that "insiders" having access to computer systems are the more likely perpetrators of fraud and abuse; that there is a proliferation of computers in government; that such security systems as currently exist do not facilitate detection of computer crimes; that security systems themselves often are vulnerable and inadequate; and that a lack of awarness and concern by the public, as well as computer systems managers, are contributing to these problems. Mr. Tompkins noted that, although the ABA did not state any formal recommendations, the conclusions reached by the respondents to the ABA survey in-

dicated: the need for Federal computer crime legislation; the need to adequately train and supervise personnel in data processing; and the large overall cost and expense of computer fraud and abuse.

Richard Kusserow, Inspector General for the Department of Health and Human Services, also testified on the nature of fraud and abuse in Federal computer systems. As Inspector General for the largest Federal civil agency, Mr. Kusserow's office has been involved with auditing computer systems, reducing costs, and insuring the integrity of HHS ADP systems. As Mr. Kusserow stated at the September 24 hearings:

> We must ensure that agency managers in overseeing programs that use computerized systems, do audit the systems, do look and make sure that the controls are functioning, and that we in the inspector general community, using our auditors and investigators, follow up to make sure it's being done. I think that in all of these areas it has not been done nearly enough.

Also, as chairman of the President's Council on Integrity and Efficiency investigating computer crime in the Federal Government, Mr. Kusserow testified on September 24, 1984, and again on October 29, 1985, on a study he directed which examined computer-related fraud and abuse in general, and a subsequent study in which the Inspector General's office interviewed those who had been convicted of Federal computer fraud and abuse. The results of these studies are consistent with the findings of the ABA study: that Federal computer fraud and abuse is often committed by insiders within the Federal agency; that training for computer security and awareness of vulnerabilities in computer systems were lacking; and that internal controls for computer security need to be increased. The profile of Federal computer criminals shows that they are young, considered good employees, and often use co-conspirators, and that many who commit these crimes never think about the consequences of being caught, or if they consider the consequences, assess the risk of being caught as minimal. As Mr. Kusserow stated in the October 29 hearing:

> One of the most disturbing findings from this study is that the work environment provided the perpetrators with the opportunity to commit their crime. We asked the perpetrators about computer security where they had committed their crime . . . Virtually all of them had been aware of security efforts but most said they had been weak. So, they made the judgment that, although there may have been security efforts in their agencies, they were weak and could not be counted upon to act as a deterrence for them to committing the crime.

The General Accounting Office also testified during the hearings on June 27, 1985, and October 29 and 30, 1985. GAO has conducted several studies on computer crime and security in the Federal Government, including a 1985 survey of 25 computer systems in 17 Federal civil agencies, to evaluate the state of computer security and integrity of these systems. This survey was conducted by GAO using two questionnaires and subsequent interviews, promising an-

onymity to the agencies so the systems could not be compromised after public disclosure. GAO indicated that:

> Generally, the results of our survey showed that each of the systems is vulnerable to abuse, destruction, error, fraud, and waste. Specifically we found that: key management responsibilities were missing. For example, many agencies do not use a risk management approach as part of implementing a security program; and actual safeguards needed to protect systems from potential threats were not always in place. For example, computerized techniques, such as passwords, allowing access to systems were not periodically changed.

GAO categorized Federal computer security methods into management and three basic safeguard components: physical, technical, and administrative. No agency met all of the management responsibilities outlined in the questionnaire, and only five of the 25 systems evaluated contained an element of physical, technical and administrative control. Only two of the systems provide what GAO described as adequate training for computer employees. GAO further characterized the systems as very vulnerable, and given the minimal oversight and coordination between agencies, GAO found that there is a lack of a balanced approach to security of Federal computer systems.

The testimony by the ABA, the Inspector General's office of HHS, and GAO clearly indicated that Federal systems are in danger because of improper use and negligence. Other witnesses from both the public and private sector testified during the hearings that they also found computer security in general and Federal computer security specifically remains vulnerable and open to fraud and abuse, despite stated efforts by representatives of the Federal agencies to remedy this problem.

ROLE OF THE NSA IN FEDERAL COMPUTER SECURITY

With the introduction of NSDD-145, the prominent role of the NSA in establishing Federal computer security in civil agencies became a subject of debate among computer security experts. The Subcommittee on Transportation, Aviation, and Materials devoted an entire day of hearings to this subject on June 27, 1985, and the role of NSA under NSDD-145 was a topic mentioned during the hearings on October 29 and 30, 1985.

Donald Latham, Chairman of the National Telecommunications and Information Systems Security Committee (NTISSC), Walter Deeley, Deputy Director for Communications Security, NSA, and Robert Brotzman, Director, DOD National Computer Security Center, testified on why NSDD-145 was necessary to coordinate Federal computer security. Citing a lack of overall coordination among Federal agencies, the high risk of compromising, losing or destroying Federal agency data, and the overall vulnerability of Federal computer security systems, they emphasized that the NSA had the experience and expertise to administer Federal computer security programs. As Mr. Latham stated:

We have provided cryptographic devices for protection of classified data, as Mr. Deeley will explain further. While we have done a reasonable job in some areas, there are still many areas that are left uncovered and there is more emphasis needed here.

We have put in controls for tighter access to unclassified data through network access controls and things like this, so that the so-called hackers can't go in and just play havoc with our data.

We are fostering very much a security awareness program. We are instituting training programs at the national level as well as the local level, I'll say, within service schools and across the various agencies. And we are looking at more rigorous ways of clearing people who have access to computer systems and telecommunications network security devices.

Other witnesses appearing before the subcommittee expressed concerns that NSDD–145 would hamper efforts to adequately administer Federal computer security. One area of concern is that NSDD–145 will create conflict with other Federal security regulations, notably Transmittal Memorandum 1 to OMB Circular A–71 (which has since been embodied in OMB Circular A–130, published December 12, 1985). Although both NSDD–145 and the OMB circular are broadly constructed, the emphasis in the OMB circular for planning and implementing Federal computer security rests with civil agencies, primarily with OMB and the Department of Commerce. In NSDD–145, the Director of NSA and the Secretary of Defense have primary roles. NSDD–145 does incorporate many of the lead Federal agencies on its NTISSC panel; but not all agencies are included. When Warren Reed, Director, Information Management and Technology Division, General Accounting Office, testified on the GAO survey on Federal computer security, he stated that the issuance of NSDD–145 might create confusion among the Federal agencies over which agency has jurisdiction over security functions. Mr. Reed stated that this could be a large or small problem, and may interfere with other Federal statutes and regulations which have given this jurisdiction to NBS. Raymond Wyrsch, Senior Attoney, Office of General Counsel at GAO, stated:

> * * * we do have laws on the books, the Brooks Act and the Paperwork Reduction Act, and there are very distinct responsibilities that have been placed on these agencies, namely OMB has been given the general oversight authority, if you will to set government policy.
>
> * * * And I don't know if anyone is really in the position to say with any degree of conclusiveness now, on what are the other agencies supposed to do if you have inconsistent or conflicting guidance that may be issued. There have been various pronouncements that have been made by the Secretary of Commerce over the years dealing with ADP standards.

Another issue regarding NSDD–145 is that of the military setting ADP security priorities for civil agencies. NTISSC has established

three levels of classifying information: classified, unclassified, and unclassified but sensitive. What information NTISSC will choose to label "unclassified but sensitive" in Federal civilian agencies is unknown.

Representative Jack Brooks, Chairman of the Subcommittee on Legislation and National Security of the House Government Operations Committee, and author of the Brooks Act, highlighted these concerns during his testimony on NSDD-145: "NSA has a propensity and a tendency to classify everything." GAO witnesses also expressed concern that a lack of definition of "unclassified information considered sensitive" in civil agencies may be interpreted either broadly or narrowly, significantly affecting how agencies store and disseminate information contained in computer and telecommunications systems. However, Lt. Gen. Odom, Director of NSA, has stated in a letter to Chairman Fuqua on February 25, 1986: ". . . the Systems Steering Group, the senior governmental body created by NSDD-145 for information security matters, has concluded that each government department or agency must make its own determination as to what constitutes sensitive information to that department or agency mission or operation."

Other witnesses, including representatives from the American Civil Liberties Union and the Institute of Electrical and Electronics Engineers, expressed similar concerns over the "unclassified but sensitive" categorization of computerized data and how that will affect citizens' access to public information or freedom to exchange scientific information.

There has been some controversy over the review process for NSDD-145. Expressing concern that issuing National Security Decision Directive 145 effectively circumvents the review process that OMB Circular A-71 went through, Subcommittee Chairman Glickman noted during testimony given on June 27, that a document which ordinarily might be called a regulation, if labeled a national security directive, may avoid the Administrative Procedures Act, all public notification requirements, and Congressional oversight. Also, Mr. Richard P. Kusserow, Inspector General of HHS, stated at the October 29 hearing that "I haven't seen it, and I have not had any imput in the process". Still the review process spanned nearly a year and Dr. Robert E. Conley, who was chairman of the Subgroup on Telecommunications Security created under NSDD-145 while he was with the Treasury Department, said at the same hearing that "we invited all of the government agencies to attend the meetings". Thus, although there is no question that Federal computer security is a vital national issue, use of NSDD-145 as an instrument for setting policy, without legislative or agency debate and review, has raised concerns in the Congress.

Although NSA has a fine track record as the lead technical agency for securing ADP systems containing national security data, it is not clear that it is the appropriate lead agency for directing civil agency computer security. Questions still remain about whether NSDD-145 will create confusion with existing Federal statutes and regulations; what the definition of "unclassified but sensitive" will mean; and whether there should be public debate and review of NSDD-145 before Congress and the Federal agencies.

TRAINING FOR FEDERAL COMPUTER SYSTEMS USERS

Testimony also described the need for greater computer security training of personnel in the Federal Government. GAO, ABA, the Inspector General of HHS, and others commented on the current state of Federal computer training and security awareness during the course of the subcommittee's hearings. Witnesses on the last day of testimony before the subcommittee on October 30, 1985, dealt directly with H.R. 2889.

H.R. 2889, as introduced by Representative Dan Glickman, would establish a focus within the Federal Government at the National Bureau of Standards for computer security research, and development of computer security training guidelines. This is to ensure that agencies would better train personnel in the vulnerabilities of computer and communication systems. The bill requires that each Federal agency provide such training on a periodic basis. The training would encompass all levels of personnel involved in the management, operation, and use of automated information processing systems.

There is little argument that such training is needed or that in some areas, that much is needed to supplement existing training procedures. Most of the witnesses testifying on the current state of Federal computer security commented that computer security training in the Federal Government is either inadequate or non-existent and that such training is necessary. William Franklin, Associate Director, Information Management and Technology Division, GAO, stated on October 30:

> There can be little question that extensive and continuing security research and training are essential if we are to gain reasonable assurance that our computerized information is properly safeguarded in storage, processing and transmission.

However, there was concern that the creation of a new structure within the Federal Government might add unnecessarily to its overall cost and bureaucracy. Several witnesses stated that existing Federal computer training facilities, such as those at NSA, should be used to train Federal employees. Robert Brotzman, Assistant Director for Computer Security at the National Computer Security Center at NSA, described the security program at the Computer Security Center. This program assists civilian and military agencies, as well as outside contractors with sensitive data, to develop secure information and communication systems. As Mr. Brotzman stated:

> The knowledge base that we have now will support an effective training program, and it will support the substantial improvement in the security of computer systems operated by and for the United States Government.

Mr. Brotzman also stated that, as introduced, H.R. 2889 might cause duplication and overlapping of effort within Federal agencies and interfere with programs already supported by NTISSC under NSDD-145.

James Burrows, Director, Institute for Computer Sciences and Technology (ICST), of the NBS, spoke on the computer training and security programs at the ICST. As part of its mandate to develop computer security standards and guidelines, the ICST assists Federal agencies in developing computer security programs. This includes both software and hardware development, system interfaces, personal identification and authentication of users. The Department of Commerce opposed the structure of H.R. 2889 because of its interpretation that the Brooks Act and other legislation makes a Federal computer training and awareness mandate for NBS unnecessary. However, Mr. Burrows did state that NSDD-145 could be "slightly confusing in who has control" of overall Federal security management among the agencies. Mr. Burrows also stated that, to date, NSDD-145 has had little adverse effect on NBS' activities in computer security and training.

Terry Culler, Associate Director, Office of Personnel Management (OPM), also spoke on H.R. 2889, stating that OPM already has the legislative authority to provide other Federal agencies with guidance on information and communication systems security training. Mr. Culler did not feel the need for the additional regulatory action, which H.R. 2889 would mandate by requiring that OPM coordinate Federal computer training. OPM currently contributes to Federal agency computer training, if the agency requests training for its employees.

Several of the witnesses did speak in favor of Federal computer training legislation, although they also suggested changes in the language and intent of H.R. 2889. Donn Parker, a computer crime and security expert at SRI International, also spoke on October 30 on computer security in general, while testifying on H.R. 2889. Mr. Parker made several observations: that it is the information, not the technology, which needs security; that information must be considered secure before it goes into the computer; that technology controls to date are adequate—it is the management of "human controls" which need improvement; that most information systems employees consider security a detriment to productivity; therefore, that measures must be taken to incorporate computer security into personnel performance evaluations; that each individual must be held accountable for taking security precautions, to ensure that these measures are taken; that advisory and counseling provisions within an organization can short-circuit the stresses and problems which may drive someone to commit a computer crime; that all information systems workers, not just computer programmers, should be trained in securing systems; and that training should be broadened to include a wider range of potential vulnerabilities, including the full civil, military, and private sector prospectives of computer training and awareness.

William Franklin of GAO also addressed H.R. 2889:

> We endorse the bill's purpose in requiring the National Bureau of Standards to establish and conduct a computer security research program in the Federal Government and the requirement that each Federal agency provide mandatory periodic training in computer security.

GAO testimony also raised the basic question of the appropriateness of a Department of Defense agency taking the lead in training civilian employees and classifying non-military, non-national security computer data. GAO supported H.R. 2889 because of the evaluation by GAO staff that H.R. 2889 clarifies the authority of NBS and its relationship to other agencies in setting training standards and computer security awareness. GAO staff expressed the opinion that such a clarification might encourage greater cooperation between NBS and NSA.

III. Need for Legislation

There are several key principles the Committee seeks to emphasize by this legislation:

1. Computer crime in the Federal Government appears to be much more pervasive and serious an issue than previously assumed. Descriptions of computer criminals as "insiders" by ABA, GAO, the Inspector General of HHS, and others may imply that many Federal computer users represent potential risks of fraud and abuse.

2. Security measures in a number of agencies are very vulnerable to abuse and fraud. Only five of 25 Federal computer systems surveyed by GAO contained minimum safeguards, and only two of 25 systems offered formal training sessions for computer users.

3. There is a need for coordinated guidance for security of sensitive information in computers. NSDD–145 further complicates a situation which already is unclear. NSDD–145 may create confusion among many Federal agencies which currently follow existing laws and regulations, such as the Brooks Act, the Paperwork Reduction Act, and the OMB circular, to set guidelines and standards for computer security.

4. NSDD–145 can be interpreted to give the national security community too great a role in setting computer security standards for civil agencies. A civilian authority is needed to develop standards relating to sensitive, but unclassified data.

5. Training of Federal personnel in ADP security is a critical issue to ensure security in Federal agencies. Yet many Federal agencies do not take advantage of available training to remedy this problem. A stronger, more active computer training and awareness program is needed to address this issue in the civil agencies of the Federal Government.

6. Greater emphasis should be given to cooperation between the military and civil agencies as well as the private sector in setting computer security and training goals. This can be accomplished by fostering greater communication and cooperation between the NBS and NSA in setting overall Federal computer policy.

IV. Explanation of the Bill

PURPOSE

The purpose of H.R. 2889, the Computer Security Act of 1986, as amended, is to improve the security and privacy of sensitive information in federal computer systems. It achieves this purpose through improved training, aimed at raising the awareness of fed-

eral workers about computer system security, by establishing a focal point within the government for developing computer system security standards and guidelines to protect sensitive information, and by requiring agencies to establish computer system security plans.

To explain what these mean, it is first necessary to examine several underlying concepts that define and scope the boundaries of the bill's coverage. First, the primary objective of the bill is controlling unauthorized use of the information in federal computer systems, rather than merely protecting the computer systems themselves. Although computer hardware and software have real value and certainly must be safeguarded, it is the data stored, manipulated, displayed and transmitted by computer systems that represent the greatest vulnerability. Nevertheless, computer systems are the instrumentality through which security measures are usually applied. Therefore, the bill makes distinctions both about which computer systems are included as well as about what kinds of information are subject to the bill's provisions.

Second, the term "computer system," as used throughout the bill, is defined broadly to include traditional computer hardware and software, and related services and other resources used in the automatic acquisition, storage, manipulation or display of information. It also includes any of the above items used in the associated electromagnetic transmission and reception of information. The word "procedures" as used in the definition is intended to include procedures for humans using the computer system. The term "federal computer system" is used to delineate the reach of the bill to include federal agencies, contractors of federal agencies and other organizations that process information using a computer system on behalf of the Federal Government to accomplish a Federal Government function. The term "operator of a federal computer system" denotes an agency or institution that owns or otherwise possesses a federal computer system, rather than an individual who physically operates the machine. Included in this definition, for example, would be state agencies that disburse federal funds or act in some other way as an extension of the federal government. The term "sensitive information" is used to limit the kinds of information which are covered by the bill. Sensitive information is defined as unclassified information which, if lost, misused, accessed or modified in an unauthorized way, could adversely affect the national interest, the conduct of federal programs or the privacy of individuals. Examples include information which if modified, destroyed or disclosed in an unauthorized manner could cause:

Loss of life;
Loss of property or funds by unlawful means;
Violation of personal privacy or civil rights;
Gaining of an unfair commercial advantage;
Loss of advanced technology, useful to a competitor; or
Disclosure of proprietary information entrusted to the government.

The definition of sensitive information allows the possibility that some unclassified information may not be sensitive. Each operator of a federal computer system must make a determination (as described later) as to which unclassified information in its possession

is sensitive. Sensitive information does not include nor does the bill apply to classified information for which extensive standards-setting authority already exists. These mechanisms are unaffected by H.R. 2889.

ADDITIONS TO NBS ORGANIC ACT

H.R. 2889 amends the Act of March 3, 1901, creating the National Bureau of Standards, to add the study of computers to the list of authorized activities of the agency. The reason for this language is to provide specific authorization for activities that are widely acknowledged as necessary in the computer age, but which are conducted currently under general authorities contained in the Act. It is intended to authorize NBS to study the means of automatic computation (computer science) independent of the technology involved. The new language is occasioned by an opportunity for legislative update, rather than being related directly to the primary purpose of the bill—computer security.

The bill also adds three new sections. Section 18 provides a hierarchical enumeration of NBS' responsibilities. At the top of the hierarchy is the mission of developing standards, and associated methods and techniques for computer systems generally. An example would be the "Open Systems Interconnection" (OSI) standards for computer networking, which the Bureau develops technically (with extensive private sector input) and presents to the American National Standards Institute, and through it to the International Standards Organization, for adoption. This statement of responsibility is intended to conform Section 18 with the above addition to the list of authorized activities.

At the next hierarchical level, NBS is responsible for developing uniform standards and guidelines, in all areas other than security, for federal computer systems. As before, this delineation of responsibility is intended to conform Section 18 and to provide specific authority for activities that are currently carried out under general provisions of the Organic Act. The product of this effort is the Federal Information Processing Standards (FIPS) which are used government-wide.

In current practice, some computer standards developed by NBS become compulsory under authority of OMB pursuant to the Brooks Act and the Paperwork Reduction Act. The process outlined in H.R. 2889—which includes standards development by NBS and subsequent promulgation by the Secretary of Commerce under redrafted authority in the Brooks Act (to be described later)—is essentially the same as current practice, but is spelled out more explicitly.

Systems involving intelligence activities, cryptologic activities related to national security, direct command and control of military forces, equipment that is integral to a weapons system or direct fulfillment of military or intelligence missions (except routine administrative and business functions) are exempted from this provision. Such systems are highly specialized in their functions and have been traditionally exempted from government-wide standards and regulations applying to general purpose computer systems. Therefore, the boundary of NBS' responsibility for non-security stand-

ards is drawn so as to exclude such defense-related, special-purpose systems.

The third hierarchial level spells out explicitly, and thereby gives special emphasis to, responsibility for standards and guidelines in the computer security arena. It assigns to NBS responsibility within the federal government for developing technical, management, physical and administrative standards and guidelines designed to achieve, in a cost-effective way, the security and privacy of sensitive information in federal computer systems. The purpose of the standards and guidelines is to control loss and unauthorized modification or disclosure of sensitive information and to prevent computer-related fraud and abuse.

Certain computer systems are exempted from this provision, regardless of the kind of information they contain. There are two categories of such exempted systems. The first is the same list of defense and intelligence-related systems that were exempted in the previous subsection, dealing with non-security standards. The second category includes systems that are operated at all times under rules designed to protect classified information. The chief effect of this exemption is to exclude classified systems from coverage by this subsection of the bill. Also exempted are mixed systems—those systems containing classified information at certain times and unclassified information at other times—provided such systems are operated at all times under the rules for protecting classified information. The purpose of this exemption is to avoid imposition of a second, less stringent set of security standards—the NBS standards—for the unclassified operations of a mixed system. Further relief for mixed systems is provided in the amendment to the Brooks Act, allowing system operators to employ standards, other than the NBS standards, if such standards are more stringent. For example, an operator of a mixed system might use a subset of the classified rules for his unclassified operations, if the subset were more stringent than the NBS standards.

The main reason for the assignment of responsibility to NBS for developing federal computer system security standards and guidelines derives from the Committee's concern about the implementation of National Security Decision Directive-145. As indicated previously, this directive established an interagency committee—the National Telecommunications and Information Systems Security Committee (NTISSC). The function of the NTISSC is to devise operating policies needed to assure the security of telecommunications and automated information systems that process and communicate both classified national security information and other sensitive government national security information. Policies developed by NTISSC would apply government-wide.

While supporting the need for a focal point to deal with the government computer security problem, the Committee is concerned about the composition of NTISSC, which favors military and intelligence agencies. It is also concerned about how broadly NTISSC might interpret its authority over "other sensitive national security information". For this reason, H.R. 2889 creates a civilian counterpart, within NBS, for setting policy with regard to unclassified information. In so doing, the bill has the additional effect of specifically limiting the purview of the NTISSC to systems containing

classified information and cancelling the authority contained in NSDD–145 for systems containing unclassified information. NBS is required to work closely with other agencies and institutions, such as NTISSC, both to avoid duplication and to assure that its standards and guidelines are consistent and compatible with standards and guidelines developed for classified systems; but the final authority for developing the standards and guidelines rests with NBS.

Note that the previous subsection dealt with developing non-security standards and guidelines, most of which affect hardware and software performance and interfaces. Accordingly, the bill's jurisdiction in that area is defined by the universe of federal computer systems, as limited by certain exceptions. In this subsection, the bill deals with security standards and guidelines, which apply more properly to protecting information. Therefore, the bill addresses unclassified (but sensitive) information in federal computer systems, but with certain systems exempted.

The method for promulgating federal computer system security standards and guidelines is the same as for non-security standards and guidelines. NBS submits them to the Secretary of Commerce along with recommendations regarding the extent to which they should be made compulsory and binding. The Secretary of Commerce, under redrafted authority in the Brooks Act (to be explained later), then promulgates standards and guidelines, making those standards compulsory and binding that he determines are necessary to improve the efficiency of operation or security and privacy of federal computer systems.

An additional responsibility of NBS is to devise guidelines for use by operators of federal computer systems containing sensitive information for their use in training their employees in security awareness and good security practice. Periodic training of this kind is required by Section 5 of H.R. 2889 to be conducted by all operators of federal computer systems that contain sensitive information.

Also, as part of its responsibility for developing computer standards and guidelines, NBS is required to devise validation procedures to evaluate the effectiveness of the standards and guidelines. This is not an enforcement or compliance determining function. Rather, it provides the ability for operators to determine if the standards and guidelines are achieving their desired purpose. NBS is to maintain liaison (as it now does) with users of the standards, to assure their workability.

Finally, in fulfilling these responsibilities, NBS is authorized to give technical assistance to the General Services Administration, the Office of Personnel Management, operators of federal computer systems and the private sector in implementing the standards and guidelines promulgated pursuant to the bill. Also, NBS is authorized to perform research and conduct studies to determine the nature and extent of the vulnerabilities of computer systems and to devise techniques to protect, in a cost effective way, the information contained in them, and to coordinate with other agencies (including NSA) which perform such research, to gain the benefits of their efforts.

A new Section 19 of the NBS Organic Act establishes a twelve-member Computer System Security and Privacy Advisory Board within the Department of Commerce. The chief purpose of the

Board is to assure that NBS receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector. Specifically, the duties of the Board are to identify emerging managerial, technical, administrative and physical safeguard issues relative to computer systems security and privacy and to advise the NBS and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems.

Members of the Board are to be appointed by the Secretary of Commerce and are to come from both inside and outside the federal government and have qualifications as specified in the bill. Members will not be paid for their services, other than for reimbursement of travel expenses. The Board may use personnel from NBS or other agencies of the federal government for the purpose of staff support, with the consent of the respective agency head.

The Board may conduct business with as few as seven members present. Findings must be reported to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of Congress.

Section 21 is a housekeeping change. It adds a short title to the NBS Organic Act for ease of reference.

AMENDMENT TO THE BROOKS ACT

H.R. 2889 contains a redrafted version of section 111(f) of the Federal Property and Administrative Services Act of 1949. The chief purpose is to establish an orderly process for promulgating standards and guidelines pertaining to Federal computer systems. Specifically, the Secretary of Commerce is charged with issuing standards and guidelines based on the standards and guidelines developed by NBS, pursuant to two subsections in the amendment to the NBS Act. As explained, those subsections formalize NBS' responsibility for developing both non-security and security standards and guidelines. The Secretary is authorized to make certain standards compulsory and binding as needed to improve the efficiency of operation or security and privacy of federal computer systems.

As described earlier, the amendment contains relief from strict compliance with these standards, when agencies already employ standards that are more stringent. An example is the instance where the unclassified operations of a mixed system are conducted under a subset of the rules used during classified operations, provided the subset is tougher than the standards mandated by the Secretary.

Further relief is provided by language authorizing the Secretary of Commerce to waive the compulsory standards when compliance would adversely affect an operator's mission or cause major financial impact on the operator that is not offset by government-wide savings. The Secretary may delegate this authority to agency heads when necessary and desirable to achieve timely and effective implementation of measures to improve federal computer system security and privacy. Agency heads may redelegate this authority only to certain high-level officials, designated pursuant to the Pa-

perwork Reduction Act for the purpose of carrying out the agencies' information management activities under that Act.

The need for delegation authority arises from Committee concerns about the administrative burden on NBS. Under normal procedures, the Secretary can be expected to rely on NBS for technical evaluation of any requests for waiver. The Committee expects NBS to devote the bulk of its energy to producing computer systems standards, rather than to such compliance determinations. Accordingly, the amendment to the Brooks Act allows the Secretary flexibility to delegate the waiver authority.

The amendment ties the process for developing and promulgating computer system standards to the requirement for an integrated information resources management system, as set forth in the Paperwork Reduction Act. To achieve this, the Administrator of General Services is charged with developing and implementing policies on federal computer systems and revising the federal information resources management regulations to reflect the standards and guidelines emanating from the Secretary of Commerce.

Finally, the amendment conforms those sections of the Brooks Act not changed by this bill by substituting the term "computer system", as defined in this bill for the terms "automatic data processing equipment" and "automatic data processing systems" wherever they appear.

TRAINING

One of the fundamental purposes of H.R. 2889 is improved computer security awareness and use of accepted computer security practice by all persons involved in management, use, or operation of federal computer systems that contain sensitive information. As indicated, the Committee found in its hearings that training in these areas is a particular weakness at most agencies. A GAO study revealed, for example, that only two of twenty-five major federal computer systems surveyed had adequate training programs. For this reason, the bill contains a requirement that each operator of a Fedeal computer system that contains sensitive information provide periodic training for its employees. The objectives of the training are to enhance employees' awareness of the threats and vulnerabilities of computer systems and to encourage the use of improved security practices.

The process envisioned in the bill starts with NBS, which is rsponsible for developing training guidelines based on its research and study of vulnerabilities and countermeasures. Within six months of enactment and using these guidelines, the Office of Personnel Management must issue regulations coverins such areas as training objectives for various categories of employee general guidance concerning course content and frequency of training. Within sixty days after OPM issues regulations, each operator must begin training of its employees, tailored to emphasize its particular operating conditions and needs. Training can be accomplished in several ways, by using the services of providers such as OPM or private companies, or by using the agencies' internal training capabilities.

SECURITY PLANS

A key determination upon which many provisions of the bill depend is the identification of which Federal computer systems contain sensitive information. By definition, the search for such systems is restricted to systems containing unclassified information. Some, but possibly not all, of these systems will be determined to contain unclassified-sensitive information. The philosophy reflected in the bill is that each Federal agency is best equipped to make that determination relative to its own mission and circumstances. Therefore, the bill calls on each agency to make a determination for each computer system under its control, within six months of enactment. The determination should be based on the definition of "sensitive" contained in the bill and use the additional guidance in the section on purpose in this report. In the case of federal contractors and other organizations, determinations are to be reviewed and approved by their supervising federal agency.

Within one year of enactment, each operator must also establish a plan for the security and privacy of each computer system so identified by the operator. Plans are to be based on the standards and guidelines issued by the Secretary of Commerce pursuant to the Brooks Act, or any waivers received. This requirement applies only to those computer systems subject to the provisions of that Act. Copies of the plans must be submitted to the National Bureau of Standards and the National Security Agency for advice and comment and to the Office of Management and Budget, which has the authority to disapprove the plan. In the case of plans established by federal contractors and other organizations, the plans are to be submitted through the supervising federal agency.

Implicit in the authority to disapprove security plans is responsibility for oversight of the identification process and compliance with the security plans as approved. Thus, OMB is the watchdog over the key implementation step in the bill.

AUTHORIZATION OF APPROPRIATIONS

The bill contains a "such sums as may be necessary" authorization for fiscal years 1987, 1988 and 1989 for each federal agency to carry out the training and planning requirements of the bill. Reauthorization will be required for subsequent years. Authorizations of appropriations needed to carry out the other provisions of the bill are implicit in the language establishing those provisions. The Congressional Budget Office has estimated this to be in the neighborhood of $20 million per year for the entire Federal government. In the case of NBS' responsibilities, explicit authorization was included in the Fiscal Year 1987 Authorization bill and must be reauthorized in future years. The CBO estimate is that $4-5 million may be required for NBS. The computer security program will, therefore, be extremely cost-effective, since testimony has indicated that losses to fraud and abuse are in excess of a billion dollars yearly.

V. Sectional Analysis—H.R. 2889

Section 1. Short Title.

Section 2. Purpose: Sets forth the Congressional declaration that

improving the security and privacy of federal computer systems is in the public interest and states Congressional intent to institute a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

The specific purposes of the Act are to assign the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems; to provide for promulgating such standards and guidelines through the Federal Property and Administrative Services Act of 1949; to require all operators of Federal computer systems that contain sensitive information to establish security plans; and to require mandatory periodic training for all persons involved in management, use or operation of Federal computer systems that contain sensitive information.

Section 3. Establishment of Computer Standards Program. Amends the Act of March 3, 1901 to add to the mission of the National Bureau of Standards the study of equipment, procedures and systems for automatic acquisition, storage, manipulation, display, and transmission of information, and its use to control machinery and processes.

Inserts a new Section 18(a) stating the National Bureau of Standards shall:

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) above, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce, for promulgation under section 111 of the Federal Property and Administrative Services Act of 1949;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security prac-

tice, as required by section 5 of the Computer Security Act of 1986; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) above through research and liaison with other government and private agencies.

Inserts a new Section 18(b) authorizing the National Bureau of Standards to:

(1) assist the private sector in using and applying the results of the programs and activities under this section;

(2) make recommendations to, assist and coordinate with other Federal agencies, as appropriate, in carrying out this Act;

(3) provide, as requested, technical assistance to operators of Federal computer systems in implementing the standards and guidelines promulgated pursuant to this Act; and

(4) perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems.

Inserts a new Section 19(a) establishing a Computer System Security and Privacy Advisory Board, with a chairman to be appointed by the Secretary of Commerce and twelve members as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

Inserts a new Section 19(b) stating that the duties of the Board shall be:

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

Inserts a new Section 19(c) stating that the term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

Inserts a new Section 19(d) prohibiting the Board from acting in the absence of a quorum, which shall consist of seven members.

Inserts a new Section 19(e) stating that Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

Inserts a new Section 19(f) that authorizes the Board in carrying out its functions, to use staff personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

Adds a new Section 20 which establishes a short title for the Act of March 3, 1901, henceforth to be known as the "National Bureau of Standards Act".

Section 4. Amendment to the Brooks Act. Replaces Section 111(f) of the Federal Property and Administrative Services Act of 1949 with new language that:

(1) empowers the Secretary of Commerce, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 18(a) (2) and (3) of the National Bureau of Standards Act, to promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems.

(2) authorizes the head of a Federal agency to employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce;

(3) provides that the standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be promptly transmitted to the Committee on Government Oper-

ations of the House of Representatives and the Committee on Governmental Affairs of the Senate; and

(4) directs the Administrator of the General Services Administration to ensure that such standards and guidelines are implemented within an integrated information resources management system (as required by chapter 35 of title 44, United States Code) by—

(A) developng and implementing policies on Federal computer systems; and

(B) revising the Federal information resources management regulations (41 CFR ch. 201) to implement such standards, guidelines, and policies.

Adds language that conforms section 111 by substituting the term "computer system" for the terms "automatic data processing equipment" and "automatic data processing systems" whenever they appear.

Section 5. Training by Operators of Federal Computer Systems. Provides that each operator of a Federal computer system that contains sensitive information shall provide mandatory periodic training in computer security awareness and accepted computer security practice. Such training shall be provided under the guidelines developed pursuant to this Act.

Training under this section shall be started within 60 days after the issuance of the regulations. Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved security practices.

Directs that within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided and the manner in which such training is to be carried out.

Section 6. Additional Responsibilities for Operators of Federal Computer Systems for Computer System Security and Privacy. Directs that within 6 months after the date of enactment of this Act, each operator of a Federal computer system shall identify each computer system, and system under development, of that operator which contains sensitive information. In the case of a Federal contractor or other organization, such identification shall be reviewed and approved by its supervising Federal agency.

Provides that within one year after the date of enactment of this Act, each such operator shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to this Act, establish a plan for the security and privacy of the identified computer systems. Copies of such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. In the case of a Federal contractor or other organization, such plan shall be transmitted through its supervising Federal agency. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget.

Section 7. Definitions. Defines—

(1) the term "computer system" as any equipment or interconnected collection of equipment, including (A) ancillary equipment, (B) software and other procedures, (C) services, and

(D) other resources that are used in the automatic acquisition, storage, manipulation, or display, or in any associated electromagnetic transmission and reception of information;

(2) the term "Federal computer system" as a computer system operated by a Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949) or by a contractor of a Federal agency or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function;

(3) the term "operator of a Federal computer system" as a Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949), contractor of a Federal agency, or other ogranization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal Government function; and

(4) the term "sensitive information" as any information, the loss, misuse, or unauthorized access or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552 of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Section 8. Authorization of Appropriations. Authorizes to be appropriated to each Federal agency such sums as may be necessary for fiscal years 1987, 1988, and 1989 to carry out the computer systems security training program established by section 5 of this Act and the indentification and planning requirements of section 6.

VI. Effect of Legislation on Inflation

In accordance with Rule XI, Clause 2(l)(4), of the Rules of the House of Representatives, this legislation is assessed to have no adverse inflationary effect on prices and costs in the operation of the national economy.

VII. Committee Oversight Findings and Recommendations

Pursuant to Rule XI, Clause 2(l)(3)(A), and under the authority of Rule X, Clause 2(b)(1) and Clause 3(f), of the Rules of the House of Representatives, the following statement on oversight activities is made:

The Committee's oversight findings are incorporated in the recommendations contained in the present bill and report.

VIII. Oversight Findings and Recommendations by the Committee on Government Operations

Pursuant to Rule XI, Clause 2(l)(3)(D), and under the authority of Rule X, Clause 2(c)(2), of the Rules of the House of Representatives, the following statement on oversight activities by the Committee on Government Operations is made:

The Committee's oversight findings are reflected in the recommendations contained in the bill as reported by that Committee and the accompanying report.

IX. Budget Analysis and Projection

The bill provides for new authorization rather than new budget authority and consequently the provisions of Section 308(a) of the Congressional Budget Act are not applicable.

X. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, June 23, 1986.

Hon. Don Fuqua,
Chairman, Committee on Science and Technology, U.S. House of Representatives, Rayburn House Office Building, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the attached cost estimate for H.R. 2889, the Computer Security Act of 1986.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,
Sincerely,

Rudolph G. Penner, *Director.*

Congressional Budget Office Cost Estimate

1. Bill number: H.R. 2889.
2. Bill title: Computer Security Act of 1986.
3. Bill status: As ordered reported by the House Committee on Science and Technology, June 4, 1986.
4. Bill purpose: H.R. 2889 would make a number of changes affecting the security of federal computer systems. It would authorize the appropriation of such sums as may be necessary for fiscal years 1987, 1988, and 1989 to carry out the planning and training programs required by the bill.

H.R. 2889 would direct the National Bureau of Standards (NBS) to establish a computer security standards program for those computer systems subject to the Brooks Act. NBS would be required to develop government-wide standards and guidelines; to conduct research; to provide technical assistance; to develop and coordinate training programs; and to develop validation standards to evaluate the effectiveness of computer security standards through research and liaison with government and private agencies. The bill would also establish a 13-member Computer System Security and Privacy Advisory Board composed of representatives of other federal agencies and the private sector.

Within six months after the date of enactment, H.R. 2889 would require all federal agencies to identify each computer that contains sensitive data. Within a year after the date of enactment, each agency would be required to establish a plan for the security for each computer and related system previously identified. The bill

would also require mandatory periodic training in computer security for all federal agency employees who manage, use or operate computer or other automated information systems. Similar training and security plans would also be required for certain employees of private contractors, and state or local governments.

5. Estimated cost to the Federal Government: CBO estimates that enactment of this bill would cost NBS about $4 million to $5 million annually beginning in 1987. Additional costs for planning and training in computer security by all agencies throughout the federal government would probably cost $20 million to $25 million in 1987 and $15 million to $20 million in each fiscal year thereafter. To the extent that this legislation would reduce fraud or other financial losses, some savings could also result from enactment of H.R. 2889. It is not possible to quantify these potential savings at this time.

Basis of estimate: Under the National Security Decision Directive (NSDD) 145, which became effective in September 1984, the President gave the National Security Agency (NSA) responsibility for ensuring the security of all classified and certain other sensitive information transmitted by federal computers or telecommunications systems. If enacted, H.R. 2889 would assign some of this authority to NBS, mainly in the area of unclassified data. Although under current guidelines it is expected that most federal agencies, with assistance from NSA, would have strengthened security efforts consistent with the directive, this bill would enhance the role of NBS and would also impose new requirements upon federal agencies and their contractors in the area of computer security.

National Bureau of Standards: Assuming enactment of H.R. 2889 by October 1, 1987, the expanded role of NBS in computer security management and training is estimated to cost about $2 million annually beginning in 1987. Based on information from NBS, an estimated $2 million to $3 million annually mayalso be needed for research, beginning in 1987. This assumes that NBS would expand its management and oversight role, but would also receive assistance and information from the National Computer Security Center (NCSC) within the Department of Defense (DoD).

Government-wide computer security plans: The level of computer security varies greatly among the approximately 80 federal entities, including about 1,300 different organizations that would be affected by this legislation. The cost of identifying all sensitive computer systems and developing an appropriate plan for facility, application and personnel security would thus vary greatly from agency to agency, depending upon the agency's current level of security, the size and number of sites, and the resources and expertise available to implement this provision.

CBO has not been able to contact each major federal entity to determine the cost of identifying and developing these plans for computer security. Based on the information available, it is expected that most agencies would probably assign existing personnel and resources to this task in order to meet the one-year deadline imposed by H.R. 2889. If approximately 10,000 plans were developed, each requiring about 1–2 work weeks of effort by agency personnel, and two and one-half work days of review by NBS, NSA, and the Office of Management and Budget (OMB), the cost spread among

the various federal agencies would be $10 million to $20 million over the fiscal years 1987 and 1988.

Government-wide training: Currently, training resources in the area of computer security are scattered throughout the federal government. A few civilian agencies, such as the Department of Energy, have developed their own computer security training for both classified and unclassified systems. Most agencies, however, send employees to commercial courses or those offered by other federal agencies, such as the General Services Administration (GSA), the Office of Personnel Management (OPM), the Department of Agriculture Graduate School, or NSA.

H.R. 2889 would require mandatory training for all federal and contractor personnel who manage, use of operate computer systems. The cost of such training depends on the number of people involved and the kind of training provided. Based on information from a number of agencies, it expected that roughly half of all government and contractor employees would initially receive some type of training as a result of the bill, or about 3 million employees. Subsequently, training would be provided to most new employees, and retraining would be required only periodically.

It is expected that most training in the area of computer security would become decentralized, with each agency responsible for developing its own programs, although some centralized training for smaller agencies and in specialized program areas would remain. The NCSC is developing a data base of educational opportunities offered by government, universities and private sources, and plans to make this available to agencies. Training courses are relatively expensive, however. They currently cost about $50 to $200 per day per person (not including development costs) and typically are offered to technical personnel who attend a three-to-five day session. In an effort to reduce training costs, NCSC is developing training packages that will be available on tape or film, sharply reducing the training cost per person.

Based on information from NCSC, GSA, OPM, and OMB, CBO made a number of assumptions about the numbers and types of training that would be required as a result of enactment of H.R. 2889. The resulting estimates provide a rough estimate of the possible additional cost of training, but should not be considered precise.

Within three years after the date of enactment, it is assumed that about 90 percent of the estimated 3 million employees affected by the bill would receive some type of computer security awareness training. Assuming the availability of training modules and other low-cost products, it is expected that the cost for this type of training would have no significant budget impact over and above the cost of maintaining good information systems, which is now the responsibility of each agency. It is estimated that about 10 percent of the 3 million employees, or 300,000, would require more formalized training. Assuming that about three-quarters of these individuals (about one-half from DoD) would have received training under current law, then about 75,000 employees would likely require training as a result of this bill. Three days of specialized training, at an average cost of $100 per day, for 75,000 persons would cost $20 million to $25 million over several years. After the initial training,

costs for retraining and training of new personnel are expected to cost about $5 million annually.

Finally, it is assumed that about 250 civilian employees would gradually be recruited and/or trained to evaluate the technical protection capabilities of industry and government-developed systems, and to train other agency personnel. This type of training, according to NCSC, takes two to three years. At an average cost of $60,000 per year, including overhead, it is estimated that this type of support staff would cost the federal government about $15 million annually, once fully implemented.

6. Estimated cost to State and local governments: H.R. 2889 would require nonfederal entities that process federal data to identify and develop security plans for each applicable computer system, and to provide security training. Based on information from Committee staff, this requirement would also apply to nonfederal entities that maintain data for ultimate federal use, or that are involved in disbursing federal funds. No complete inventory of the relevant systems currently exists, and it is not possible at this time to estimate with precision the costs to state and local governments. Based on the limited information available, we expect that total costs incurred by state and local governments are likely to be less than $25 million annually.

7. Estimate comparison: None.

8. Previous CBO estimate: On November 14, 1985, CBO prepared a cost estimate for H.R. 2889, as ordered reported by the House Committee on Government Operations. The estimated costs of this version of H.R. 2889 reflect a later assumed date of enactment.

9. Estimate prepared by: Mary Maginniss.

10. Estimate approved by: C.G. Nuckols (for James L. Blum, Assistant Director for Budget Analysis).

XI. Changes in Existing Law Made by the Bill, As Reported

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

Act of March 3, 1901

AN ACT To establish the National Bureau of Standards

* * * * * * *

Sec. 2. The Secretary of Commerce (hereinafter referred to as the "Secretary") is authorized to undertake the following functions:

(a) * * *

* * * * * * *

(f) Invention and development of devices to serve special needs of the Government.

In carrying out the functions enumerated in this section, the Secretary is authorized to undertake the following activities and similar ones for which need may arise in the operations of Government agencies, scientific institutions, and industrial enterprises:

(1) * * *

* * * * * * *

(18) the prosecution of such research in engineering, mathematics, and the physical sciences as may be necessary to obtain basic data pertinent to the functions specified herein; [and]

(19) the compilation and publication of general scienctific and technical data resulting from the performance of the functions specified herein or from other sources when such data are of importance to scientific or manufacturing interests or to the general public, and are not available elsewhere, including demonstration of the results of the Bureau's work by exhibits or otherwise as may be deemed most effective, and including the use of National Bureau of Standards scientific or technical personnel for part-time or intermittent teaching and training activities at educational institutions of higher learning as part of and incidental to their official duties and without additional compensation other than that provided by law[.];

(20) the study of equipment, procedures, and systems for automatic acquisition, storage, manipulation, display, and transmission of information, and its use to control machinery and processes.

* * * * * * *

SEC. 18. (a) The National Bureau of Standards shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

(4) Submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce, for promulga-

tion under section 111 of the Federal Property and Administrative Services Act of 1949;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1986; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

(1) to assist the private sector in using and applying the results of the programs and activities under this section;

(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949;

(3) as required, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949;

(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1986;

(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

(c) As used in this section and section 19, the terms "computer system", "Federal computer system", "operator of a Federal computer system", and "sensitive information" have the meanings given in section 7 of the Computer Security Act of 1986.

SEC. 19. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the

Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommuncations equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

(b) The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

(c) The term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

SEC. [18.] *20.* Appropriations to carry out the provisions of this Act may remain available for obligation and expenditure for such period or periods as may be specified in the Acts making such appropriations.

SEC. 21. This Act may be cited as the National Bureau of Standards Act.

SECTION 111 OF THE FEDERAL PROPERTY AND ADMINISTRATIVE SERVICES ACT OF 1949

AUTOMATIC DATA PROCESSING EQUIPMENT

SEC. 111. (a) The Administrator is authorized and directed to coordinate and provide for the economic and efficient purchase, lease, and maintenance of [automatic data processing equipment] *Computer systems* by Federal agencies.

(b)(1) [Automatic data processing equipment] *computer systems* suitable for efficient and effective use by Federal agencies shall be provided by the Administrator through purchase, lease, transfer of equipment from other Federal agencies, or otherwise, and the Administrator is authorized and directed to provide by contract or otherwise for the maintenance and repair of such equipment. In carrying out his responsibilities under this section the Administrator is authorized to transfer [automatic data processing equipment] *computer systems* between Federal agencies, to provide for joint utilization of such equipment by two or more Federal agencies, and to establish and operate equipment pools and data processing centers for the use of two or more such agencies when necessary for its most efficient and effective utilization.

(2) The Administrator may delegate to one or more Federal agencies authority to operate [automatic data processing equipment] *computer systems* pools and automatic data processing centers, and to lease, purchase, or maintain individual [automatic data processing systems] *computer systems* or specific units of equipment, including such equipment used in automatic data processing pools and automatic data procesing centers, when such action is determined by the Administrator to be necessary for the economy and efficiency of operations, or when such action is essential to national defense or national security. The Administrator may delegate to one or more Federal agencies authority to lease, purchase, or maintain [automatic data processing equipment] *computer systems* to the extent to which he determines such action to be necessary and desirable to allow for the orderly implementation of a program for the utilization of such equipment.

* * * * * * *

[(f) The Secretary of Commerce is authorized (1) to provide agencies, and the Administrator of General Services in the exercise of the authority delegated in this section, with scientific and technological advisory services relating to automatic data processing and related systems, and (2) to make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards. The Secretary of Commerce is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems, as may be required under provisions of this subsection.]

(f)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 18(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to im-

prove the efficiency of operation or security and privacy of Federal computer systems.

(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversly affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be promptly transmitted to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate.

(4) The Administrator shall ensure that such standards and guidelines are implemented within an integrated information resources management system (as required by chapter 35 of title 44, United States Code) by —

(A) developing and implementing policies on Federal computer systems; and

(B) revising the Federal information resources management regulations (41 CFR ch. 201) to implement such standards, guidelines, and policies.

(5) As used in this section, the terms "computer system", "operator of a Federal computer system", and "Federal computer system" have the meanings given in section 7 of the Computer Security Act of 1986.

(g) The authority conferred upon the Administrator and the Secretary of Commerce by this section shall be exercised subject to direction by the President and to fiscal and policy control exercised by the Office of Management & Budget. Authority so conferred upon the Administrator shall not be so construed as to impair or interfere with the determination by agencies of their individual [automatic data processing equipment] *computer systems* requirements, including the development of specifications for and the selection of the types and configurations of equipment needed. The Administrator shall not interfere with, or attempt to control in any way, the use made of [automatic data processing equipment] *computer systems* or components thereof by any agency. The Administrator shall provide adequate notice to all agencies and other users concerned with respect to each proposed determination specifically affecting them or the [automatic data processing equipment] *computer systems* or components used by them. In the absence of

mutual agreement between the Administrator and the agency or user concerned, such proposed determinations shall be subject to review and decision by the Office of Management & Budget unless the President otherwise directs.

* * * * * * *

XII. Committee Recommendation

A quorum being present, the bill was ordered favorably reported on June 4, 1986 by unanimous voice vote.

XIII. ADDITIONAL VIEWS FOR H.R. 2889, COMPUTER SECURITY REPORT

We are sensitive to the Administration's concerns about this bill. We believe we have reached a compromise that, while far from perfect, gives directors of agencies the discretion they need to implement reasonable, effective security procedures.

For example, agency directors are given the option of choosing a single standard for their agency rather than being required to handle different data in different ways.

Our goal has been to give agency directors maximum flexibility to enable them to decide the type of security system needed to protect sensitive government information.

SHERWOOD L. BOEHLERT.
MANUEL LUJAN, Jr.
TOM LEWIS.
RON PACKARD.

XIV. DISSENTING VIEWS FOR H.R. 2889, COMPUTER SECURITY REPORT

We are opposed to H R. 2889 as reported by the Committee. This unnecessary, ill-timed effort to pre-empt Administration policy is likely to lead only to confusion and duplication of efforts.

This bill's supporters claim the measure is needed because National Security Decision Directive (NSDD)–145 will give the National Security Agency control over how civilian agencies operate their computer systems. Yet there is no evidence of any interference by NSA in civilian agencies. Indeed, civilian agencies are represented on the National Telecommunications and Information Systems Security Committee (NTISSC), which is in the process of formulating security guidelines. There is no reason to pre-empt the panel's work.

H.R. 2889 also provides for security training by the National Bureau of Standards. However, NSA already is putting out training material. A new efffort by the Bureau could easily lead to pointless duplication.

We ought to give NSDD–145 a chance to work before we begin tinkering.

F. JAMES SENSENBRENNER, Jr.
DON RITTER.
JOE BARTON.
DAVID S. MONSON.

○